US, Taiwan, India join forces against China cybersecurity threat

AJAI SHUKLA
New Delhi, 13 December

PHOTO: X/US AMBASSADOR ERIC GARCETTI

United States (US) Ambassador Eric Garcetti said that the US is committed to working closely with partners like India and Taiwan to enhance cybersecurity and protect shared interests in the digital space

With China looming ever larger as a potent cyber threat, American, Indian and Taiwanese cybersecurity officials have met to find ways of deepening their operational expertise and sharing best practices on cybersecurity issues.

The meeting took place on Monday and Tuesday during a joint workshop convened under the Global Cooperation and Training Framework (GCTF). This was the first in-person GCTF programme held in India. Co-hosting the event were US Ambassador to India Eric Garcetti, Taiwan's Representative to India, Baushuan Ger, India's former National Cyber Security Coordinator, Lieutenant General Rajesh Pant, and the Indian government-sponsored think tank, United Service Institution of India (USI).

All three countries share a common interest in warding off cyber attacks from various agencies that the People's Liberation Army (PLA) is developing and training in China.

Ambassador Garcetti said, "The United States is committed to working closely with partners like India and Taiwan to enhance cybersecurity and protect our shared interests in the digital space. When we connect, protect, and detect with technology, instead of fearing what it can do to divide or oppress us, we can take full advantage of the nearly limitless potential that these advances will bring."

Pant said India, with over 800 million internet users and 1.2 billion smartphones, regarded cybersecurity as a major component of national security.

NEWS ANALYSIS

The Defence Cyber Agency (DCyA) is a tri-service command of the Indian military. Headquartered in New Delhi, the agency is tasked with handling and defeating cyber security threats.

The DCyA draws personnel from all three branches of the Indian military. The DCyA head is a two-star rank officer who reports to the CDS through the Integrated Defence Staff (IDS).

A two-star admiral, Mohit Gupta, was appointed in May 2019 as the first head of the DCyA. As of 2021, the DCyA was fully operational with the army, navy and IAF establishing their respective Cyber Emergency Response Teams (CERT).

The Naresh Chandra Task Force (NCTF) was set up in July 2011 by then National Security Advisor Shivshankar Menon to review the recommendations of the Kargil Review Committee, assess the implementation progress, and suggest new reforms related to national security. The NCTF was led by retired bureaucrat Naresh Chandra and comprised 13 other members.

Among its recommendations, the Task Force recommended the creation of a cyber command (DCyA), an aerospace command and a special operations command. All three were proposed to be tri-service commands in order to bring the various special forces units of the military under a unified command and control structure.

Representative Ger highlighted GCTF's importance as a platform to utilise Taiwan's strengths in addressing issues of global concern.

The US is widely regarded as the world's premier cyber warfare superpower. The US Army Cyber Command integrates and conducts cyberspace operations, electromagnetic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information dimension while denying the same to our adversaries.

The US Army Cyber Command (ARCYBER) is the supporting Army headquarters under the United States Cyber Command.

"We operate and defend Army networks and deliver cyberspace effects against adversaries to defend the nation with over 16,500 soldiers, civilians, and contractors working 24/7 across the globe," says the US Cyber Command.

According to ARCYBER, its more critical and complex priority is to operate and aggressively defend the Department of Defense Information Network.

The ARCYBER says its most critical ability is to deliver cyberspace effects – both defensive and offensive – against global adversaries. Towards this, the US military believes it must equip its forces for the future fight against a resilient, adaptive adversary.

ARCYBER is regarded as engaged in the real-world cyberspace fight today, against near-peer adversaries, and other global cyber threats. According to ARCYBER: "We defend military networks, secure Army weapons platforms, and protect critical US infrastructure. Army Cyber forces are deployed globally, conducting defensive and offensive cyber operations 24/7."

Since its launch in 2015, the GCTF has held 70 international workshops with participation from over 120 countries to strengthen connections among experts on public health, supply chains, humanitarian assistance, digital health and other regional issues.

The US, Taiwan, the Australian Office, Taipei, and the Japan-Taiwan Exchange Association jointly administer the GCTF, which serves as a platform for Taiwan to share its expertise with partners around the world.

"The United States looks forward to continued collaboration with India, Taiwan, and like-minded partners to tackle shared challenges," says ARCYBER.

Taiwan has world-class experts in a wide variety of fields, including public health, law enforcement, disaster relief, energy cooperation, women's empowerment, digital economy and cyber security, media literacy, and good governance.

However, pressure from Beijing prevents many international institutions from allowing Taiwan to participate.Consequently, Taiwan's experts are not able to share their knowledge. The GCTF allows practitioners from around the world to learn what Taiwan has to offer and to strengthen connections between experts in different countries as they tackle 21st-century problems that do not respect borders.